NORTH-HOLLAND

Perfect Sumsets in Finite Abelian Groups

Aart Blokhuis and Henny A. Wilbrink
Technical University Eindhoven
P.O. Box 513
5600 MB Eindhoven
The Netherlands

and

Attila Sali*
Mathematical Institute of HAS
Budapest P.O. Box 127
H-1364 Hungary

Dedicated to J. J. Seidel

Submitted by Willem Haemers

ABSTRACT

We prove that if G is a finite abelian group of odd order n and $A \subset G$ is of size a such that for every $g \in G$ there exist $u, v \in A$ with $g = u + v$, then $n \leqslant [(a-1)^2 + 1]/2$ if a is even and $n \leqslant [(a-1)^2 + 2]/2$ if a is odd. We show that equality occurs if and only if $n \in \{3, 5, 9, 13, 25, 243\}$.

1. INTRODUCTION

G. Ebert asked how large a set of points in $AG(2, q)$ must be if it determines all possible directions of the affine plane. One possible construction is taking a set of points $\{(t, t^2) : t \in T\}$ for some suitably chosen T. Then the directions determined by this point set are exactly the numbers $t + u$ for

* This research was done while the third author visited the Technical University of Eindhoven. Research was partially supported by Hungarian National Research Fund Grant No. 4267.

655 Avenue of the Americas, New York, NY 10010
0024-3795/95/$9.50
SSDI 0024-3795(95)00232-3

$t, u \in T$. Thus, the question arises: what is the minimum subset A of Z_p^n such that each r can be written in at least one way as $r \equiv u + v \pmod{n}$ with $u, v \in A$? Graham and Sloane [3] investigate the sort of "dual" problem. They define $n_\gamma(k)$ as the largest number n such that there exists a subset $A = \{0 = a_1 < a_2 < \cdots < a_k\}$ of the residue classes modulo n with the above property. They show using methods of Hämmerer and Hofmeister [4] that

$$\tfrac{5}{18}(k-1)^2 < n_\gamma(k) < \tfrac{1}{2}k^2 + O(k).$$

Their upper bound follows from the trivial observation that $n \leqslant \binom{k}{2}$. Equality would occur if all pairwise sums of elements of A were different. That would imply all pairwise differences are distinct. However, there are $k(k-1)$ possible pairwise differences, thus equality cannot hold.

On the other hand, it is quite natural to extend the scope of investigations from cyclic groups to arbitrary finite abelian groups. Using the above observation about pairwise differences, we first show the following.

PROPOSITION 1.1. *Let G be a finite abelian group of odd order n. Assume that $A \subset G$ satisfies the condition that every element $g \in G$ can be written as $g = u + v$ with $u \neq v$ elements of A. Put $|A| = a$. Then*

$$n \leqslant \begin{cases} \dfrac{(a-1)^2 + 1}{2} & \text{if } a \text{ is even}, \\ \dfrac{(a-1)^2 + 2}{2} & \text{if } a \text{ is odd}. \end{cases}$$

Next we introduce the notion of perfect sumset.

DEFINITION 1.2. If G and A are as in Proposition 1.1 and equality holds, then A is called a perfect *sumset* in G.

The first question is whether perfect sumsets exist. The trivial example of $\mathbf{Z}_3$ with $a = n = 3$ shows that they exist, indeed. Our main theorem answers the next natural question.

THEOREM 1.3. *If G is a finite abelian group of odd order n and a perfect sumset exists in G, then $n \in \{3, 5, 9, 13, 25, 243\}$. Furthermore, there are examples of perfect sumsets for each particular n in the above list and every such example is isomorphic to one of those listed in Section 3.*

In the next section we present the proofs, and we show the examples in Section 3. The proof of Theorem 1.3 requires solution of several Diophantine equations. These are quite standard and we have put them into an appendix.

2. PROOFS

Usually we consider unordered pairs of elements of A, when we work with sums. However, the following proof is an exception.

Proof of Proposition 1.1

Let s_i denote the number of elements $g \in G$ such that there exist exactly i *ordered* pairs of not necessarily distinct elements $(u, v) \in A \times A$ with $g = u + v$. Similarly, let d_i be the number of elements $g \in G$ such that there exist exactly i pairs $(u, v) \in A \times A$ with $g = u - v$. Note that $s_0 = s_1 = 0$ and $d_a \geqslant 1$. Counting the number of elements of G, $A \times A$ and the elements (u, v, w, x) of $A \times A \times A \times A$ such that $u + v = w + x$, respectively, we obtain the following sets of equations:

$$\sum s_i = n, \qquad \sum d_i = n,$$

$$\sum i s_i = a^2, \qquad \sum i d_i = a^2,$$

$$\sum i^2 s_i = q, \qquad \sum i^2 d_i = q.$$

The last pair of equations is true, because we can make a one-to-one correspondence φ between the 4-tuples (a, b, c, d) with property $a + b = c + d$ and 4-tuples (x, y, z, t) with property $x - y = z - t$ by $\varphi((a, b, c, d)) = (a, c, d, b)$. We shall bound q from below and above. First, let us observe that $d_a \geqslant 1$, since 0 occurs as a difference a times. Hence

$$\sum (i - 2)(i - 3) d_i \geqslant (a - 2)(a - 3),$$

or

$$q \geqslant 6a^2 - 5a - 6n + 6.$$

On the other hand, every element of the form $2x$ for $x \in A$ occurs an odd number of times as a sum, so the sum of s_i's for odd indices is exactly a. It follows that $\sum (i-2)(i-a)s_i \leqslant (3-a)a$ if a is even, and $\leqslant (3-a)(a-1)$ if a is odd. For q, this gives (with $\varepsilon = 1$ if a is odd, and 0 if a is even):

$$q \leqslant (a+2)a^2 - 2an + (3-a)(a-\varepsilon).$$

Combining upper and lower bounds for q, we get

$$(a-3)(a^2 - 2a + 2 + \varepsilon - 2n) \geqslant 0,$$

giving the desired inequalities. ■

Proof of Theorem 1.3

The proof of Proposition 1.1 shows that if $A \subset G$ is a perfect sumset, then there exists an element g of G such that g occurs as a sum $a/2$ or $(a-1)/2$ times depending on the parity of a, and all the other elements of G occur exactly once. By a simple translation, we may assume that 0 occurs many times. This immediately leads to the following.

STEP 1. $x \in A \Leftrightarrow -x \in A$.

The next step is the most important in the characterization.

STEP 2. $x \in A$ implies that $3x \in A$.

Indeed, $2x$ has to be a sum of two elements of A, say $2x = y + z$. This implies $x - y = z - x$. However, $-y, -x \in A$ by Step 1, so we have two pairs from A with the same sum. This sum cannot be 0, because that would imply $x = y = z$, so the two pairs cannot be different, i.e, $\{x, -y\} = \{z, -x\}$, or the two elements in one of the pairs are the same, say $x = -y$. The first case again would imply $x = y = z$, so we have $x = -y$, consequently $z = 3x$.

STEP 3. If 3 does not divide the order of G, then G is an elementary abelian 5-group or $a = 6$.

For the proof of Step 3 we consider G in multiplicative form, and construct the group ring $\mathbf{F}_3[G]$ with coefficients from the 3-element field. In this ring we identify $U = \{u_1, u_2, \ldots, u_t\} \subset G$ with $u_1 + u_2 + \cdots + u_t \in \mathbf{F}_3[G]$. Let $A^{(i)} = \sum_{x \in A} x^i$. Let us first assume that a is even. Then by the perfect sumset property, we have

$$A^2 = 2G + (a-2)1 + A^{(2)}.$$

In $\mathbf{F}_3[G]$ we have $A^3 = A^{(3)}$, but by Step 2 and the fact that 3 is not a divisor of $|G|$, we obtain that $A^{(3)} = A$. Thus, $A^4 = A^2$, so $A^2 = 2G + (a-2)1 + A^{(2)}$ is an idempotent in $\mathbf{F}_3[G]$. However, $A^{(2)}$ is also a perfect sumset with 0 occurring as a sum many times, so we can conclude that $2G + (a-2)1 + A$ is an idempotent

$$(2G + (a-2)1 + A)^2 = 2G + (a-2)1 + A.$$

This implies

$$(2a^2 + 4a - 4)G + (a-2)^2 1 + A^{(2)} + (2a-5)A = 0.$$

If $a \equiv 1 \pmod 3$, then we have $A^{(2)} = G - 1$, which implies $a = n - 1 = 4$. If $a \equiv 0 \pmod 3$, then the above equation reads $A^{(2)} + A = G - 1$, i.e., $2a = n - 1$, so $a = 6$. Finally, if $a \equiv -1 \pmod 3$, we obtain $A^{(2)} = A$, which means (returning to the additive writing of G) that $x \in A$ implies that $2x \in A$. So, if $x \in A$, then $\{\ldots, -2x, -x, x, 2x, 3x, 6x, \ldots\} \subset A$. However, now we can write $4x$ in two ways, namely, $4x = x + 3x = 6x + (-2x)$. This implies that $6x = x$, i.e.,

$$5x = 0 \quad \text{for } x \in A.$$

From this immediately follows that every element of G is of order 5. The case a is odd can be treated in a similar way.

STEP 4. If G is an elementary abelian 5-group, then $|G| = 5$ or $|G| = 25$.

We have that $n = 5^m$ for some m. Expressing n with a, we obtain

$$\frac{(a-1)^2 + 1}{2} = 5^m.$$

The case a is odd cannot occur, because $[(a-1)^2+2]/2$ is never divisible by 5. The only solutions of the above equation are $a=4$, $m=1$ and $a=8$, $m=2$ (see the appendix).

It follows from the above that if $3 \nmid |G|$, then $|G|$ is 5, 13, or 25.

STEP 5. If $3 \mid n$, then G is a 3-group.

Note that in this case a must be odd, because $[(a-1)^2+1]/2$ is never divisible by 3. Let $G = U \times V$ where U is a 3-group and $3 \nmid |V|$. If $(x, y) \in A$, then, multiplying by 3 enough times, we obtain $(0, y) \in A$. Thus, the set $B = \{y : (0, y) \in A\}$ is a perfect sumset in V. However, $|B|$ is odd, while by the above steps a perfect sumset in group whose order is not divisible by 3 must be even.

The only thing remaining to finish the proof is the following.

STEP 6. If G is a 3-group, then $n = 3$, 9, or 243.

As we have seen before, a must be odd, so $n = [(a-1)^2+2]/2$. Again, we have to solve a Diophantine equation

$$\frac{(a-1)^2+2}{2} = 3^m.$$

The only solutions are $m = 1, 2, 5$ (see [2] or the Appendix). ■

3. EXAMPLES

In each of the examples below it is straightforward to check that the given A is a perfect sumset. One only has to check that the sizes are right and that every element of the given G is a sum of two different elements of A.

$\boldsymbol{n = 3}$ Here we take $A = G = \mathbf{Z}_3$.

$\boldsymbol{n = 5}$ Again, there is only one group, $G = \mathbf{Z}_5$. A has to be of size 4, so for example, $A = G \setminus \{0\}$ is good.

$\boldsymbol{n = 9}$ Let us first take $G = \mathbf{Z}_9$, then $A = \{0, 1, 3, 6, 8\}$ works. If we take $G = \mathbf{Z}_3 \times \mathbf{Z}_3$, then $A = \{(0,0), (1,1), (1,2), (2,1), (2,2)\}$ is a perfect sumset in G.

$\boldsymbol{n = 13}$ Taking $A = \{1, 3, 4, 9, 10, 12\}$ or $2A$ in $\mathbf{Z}_{13}$, we obtain a perfect sumset. On the other hand, by the argument of Step 3 we see that A and $2A$

together must cover all nonzero elements. This implies that they must be disjoint, so the above two are the only cases when 0 occurs many times as a sum. They are isomorphic, so up to isomorphism, there is only one perfect sumset in $\mathbf{Z}_{13}$.

$\boldsymbol{n = 25}$ According to Step 3, we need to consider $G = \mathbf{Z}_5 \times \mathbf{Z}_5$. Now

$$A = \{(1,0),(2,0),(3,0),(4,0),(1,1),(2,2),(3,3),(4,4)\},$$

which is equivalent to the set $\{x \in \mathbf{F}_{25} : x^8 = 1\}$, works.

$\boldsymbol{n = 243}$ Take G to be the additive group of $GF(3^5)$, that is $(\mathbf{Z}_3)^5$. Choose A to be the collection of 11th powers in GF (243).

We can characterize the perfect sumsets in the $n = 243$, as well.

PROPOSITION 3.1. *If* $n = 243$, *then* $G = (\mathbf{Z}_3)^5$.

Proof of Proposition 3.1

Let us consider G to be in multiplicative form again, and use the group ring $\mathbf{F}_3[G]$. We do not distinguish between subsets of G and the sum of elements of subsets, considered as being an element of $\mathbf{F}_3[G]$. We have in this ring that $A^2 = 2G + (a - 3)1 + A^{(2)}$. Using that $A^{(2)}$ is a perfect sumset and that $a \equiv 2 \pmod 3$, we obtain that

$$A^4 = \left(A^2\right)^2 = A^{(4)} + A^{(2)} = A^3A = A^{(3)}A.$$

By the perfect sumset property and the fact that $A^{(3)} \subset A$, the number of elements with nonzero coefficients on the right-hand side is at least $|A^{(3)}|(a - |A^{(3)}|)$. On the other hand, the number of elements with nonzero coefficients in $A^{(4)} + A^{(2)}$ is at most $2a - 1$. Thus, $|A^{(3)}| \leqslant 2$. If there are two elements in $A^{(3)}$ with nonzero coefficients, then they must by y and y^{-1} for some $y \neq 1$. So, the coefficient of 1 is zero, i.e., we have an element $x \in A$ such that $x^3 = 1$. However, in this case $\{1, x, x^{-1}\} \subset A^{(4)} \cap A^{(2)}$, so the number of different elements with nonzero coefficients on the left-hand side is at most $2a - 3$, a contradiction. The sum of coefficients in $A^{(3)}$ is congruent 2 modulo 3, hence we have exactly one element with nonzero coefficient. This can only be 1, consequently every element in A is of order 3, i.e., every element of G is of order 3. ■

We can construct the unique perfect 2-error correcting code of dimension 6 in $(\mathbf{F}_3)^{11}$ from a perfect sumset in $(\mathbf{Z}_3)^5$, as follows. We take the nonzero

elements of A as column vectors and choose one from each $x, -x$ pair. In this way we obtain 11 vectors that form a 5×11 matrix. We claim that if there is a linear dependency among some columns of this matrix, then at least five columns are involved. Note that the coefficients in a linear combination can only be ± 1. Indeed, columns are nonzero, so at least two are needed. But if two were dependent, say x and y, then we would have $x = -y$, contradicting the choice of vectors. If three were dependent, then we would have $x = y \pm z$, which means x is realized in two different ways as a sum: $x = x + 0$ and $x = y \pm z$. Similarly, a four-term dependence would mean $0 \neq x \pm y = z \pm v$, and that again contradicts the perfect sumset property. Thus, the dual code generated by this matrix has minimum distance 5, dimension 6, so it must be the perfect 2-error correcting ternary (Golay) code. This completes the characterization of the perfect sumsets for $n = 243$.

4. APPENDIX

PROPOSITION 4.1. *The only solutions of the equation*

$$x^2 + 1 = 2 \cdot 5^m$$

are $(x, m) = (1, 0), (3, 1), (7, 2)$.

Proof of Proposition 4.1

We shall consider two Pell-equations, according to the parity of m, namely, $x^1 - 2y^2 = -1$ and $x^2 - 10y^2 = -1$, where y must be a power of 5.

Case 1. The basic solution of the first equation is $x = y = 1$, so any other solution is of the form

$$x + y\sqrt{2} = \pm\left(1 + \sqrt{2}\right)^{2k+1}.$$

This can be written as

$$x + y\sqrt{2} = \pm\left(7 + 5\sqrt{2}\right)^r\left(1 + \sqrt{2}\right)^{\varepsilon}, \tag{1}$$

where $\varepsilon = 0, 1, 2$. Considering (1) modulo 5, the left-hand side is x unless $y = 1$, because y is a power of 5. The right-hand side is $7^r\,(1 + \sqrt{2})^{\varepsilon}$. x is a

rational integer, so $\varepsilon = 0$, consequently $r = 2k + 1$. This yields that

$$y = \pm \sum_{i=0}^{k} \binom{2k+1}{2i+1} 5^{2i+1} 2^i 7^{2k-2i}. \tag{2}$$

We claim that (2) is not a power of 5 unless $k = 0$. Indeed, if $2k + 1 = 5^t z$, where z is not divisible by 5, then the $i = 0$ term of the r.h.s. of (2) is divisible by exactly 5^{t+1}. On the other hand, the exponent of 5 in the remaining terms is at least $t + 2i + 1 - u$, where u is the exponent of 5 in $(2i + 1)!$. However, it is elementary to see that $u < 2i - 1$ if $i > 0$.

Case 2. The basic solution of the second equation is $x = 3$ and $y = 1$. Now

$$y = \pm \sum_{i=0}^{k} \binom{2k+1}{2i+1} 9^{k-i} 10^i. \tag{3}$$

Similarly to the previous case, we get that the $i = 0$ term of the r.h.s. of (3) is divisible by a strictly smaller power of 5 than the rest, using that the largest power of 5 that divides $(2i + 1)!$ is at most $\lfloor (2i + 1)/4 \rfloor$. ■

PROPOSITION 4.2. *The only solutions of the equation*

$$1 + 2x^2 = 3^n$$

are $(x, n) = (0, 0), (1, 1), (2, 2)$ *and* $(11, 5)$.

We just give a sketch of the proof of Proposition 4.2. For more details see [1, 2].

1. Factorization in $\mathbf{Q}\sqrt{-2}$ *(this is a UFD):*

$$(1 + x\sqrt{-2})(1 - x\sqrt{-2}) = (1 + \sqrt{-2})^n (1 - \sqrt{-2})^n.$$

2. $\gcd(1 + x\sqrt{-2}, 1 - x\sqrt{-2}) = 1$, since it divides 2 and $1 + 2x^2$, so without loss of generality, $1 + x\sqrt{-2} = \pm(1 + \sqrt{-2})^n$, from which it follows that

$$(1 + \sqrt{-2})^n + (1 - \sqrt{-2})^n = \pm 2. \tag{4}$$

3. Consider (4) mod 3^7 with $\sqrt{-2} = 508$: Solutions are $n = 0, 1, 2, 5$ or $n = 86 \pmod{3^6}$.

4. Consider (4) mod 1459 with $\sqrt{-2} = 54$: OK for $n = 0, 1, 2, 5$ (of course), but for $n = 86 + 729k$, we get

$$55^{86+729k} + (-53)^{86+729k} = 353 + (1)^k 864 \neq \pm 2 \pmod{1459}.$$

■

REFERENCES

1 L. E. Dickson, *History of the Theory of Numbers Vol. 2*, Chelsea Publishing Company, New York, 1966, p. 694.
2 E. Fauquembergue, *Mathesis (2)*, 4:160–170 (1894).
3 R. L. Graham and N. J. A. Sloane, On additive bases and harmonious graphs, *SIAM J. Alg. Discrete Meth.* 1:382–404 (1980).
4 N. Hämmerer and G. Hofmeister, Zu einer Vermutung von Rohrbach, *J. reine angew. Math.* 286/287:239–247 (1976).

Received 7 July 1994; final manuscript accepted 29 September 1994